Congruences : résumé

Définition : soient a, b et n trois entiers relatifs. On dit que a est congru à b modulo n, ce que l'on note $a \equiv b\ [n]$ ou $a \equiv b\ (\mathrm{mod}\ n)$, lorsque n divise $a - b$.

Remarques : • n divise a si et seulement si $a \equiv 0\ [n]$.
• On a $a \equiv a\ [n]$ (réflexivité)
• $a \equiv b\ [n] \iff b \equiv a\ [n]$ (symétrie)

Propriété : soit $n \in \mathbb{N}^*$ et a, b dans $\mathbb{Z}$; alors $a \equiv b\ [n]$ si et seulement si a et b ont le même reste dans leur division euclidienne par n.

Remarque : si $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$, il existe un unique entier r dans $\{0; 1; \cdots; n-1\}$ tel que $a \equiv r\ [n]$: il s'agit du reste r de la division euclidienne de a par n.

Propriétés : soient a, b, c et d des entiers relatifs, et $n \in \mathbb{N}^*$.
1) Si $a \equiv b\ [n]$ et $k \in \mathbb{Z}$, alors $k \times a \equiv k \times b\ [n]$.
2) Si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, alors $a \equiv c\ [n]$ (transitivité de $\equiv$).
3) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a + c \equiv b + d\ [n]$ (compatibilité de $\equiv$ avec $+$).
4) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a - c \equiv b - d\ [n]$ (compatibilité de $\equiv$ avec $-$).
5) Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors $a \times c \equiv b \times d\ [n]$ (compatibilité de $\equiv$ avec $\times$).

Remarque : grâce à la prop. 5, la relation $\equiv$ est également compatible avec l'élévation à la puissance (exposant positif !) $\longrightarrow$ si $a \equiv b\ [n]$, on a pour tout $k \in \mathbb{N}^*$, $a^k \equiv b^k\ [n]$.

Exercices résolus :
1) Déterminer le reste dans la division euclidienne de 44^{1000} par 7.
2) Prouver que pour tout entier naturel n impair, $15^n + 2017$ est divisible par 16.

↪ **Solutions :**
1) On a $44 \equiv 2\ [7]$ donc $44^{1000} \equiv 2^{1000}\ [7]$. Remarquons que $2^3 \equiv 1\ [7]$, donc $(2^3)^{333} \equiv 1^{333}\ [7]$, soit $2^{999} \equiv 1\ [7]$, d'où $2^{1000} \equiv 2\ [7]$. On en déduit que $44^{1000} \equiv 2\ [7]$; le reste cherché est donc 2.

2) On a $15 \equiv -1\ [16]$, donc $15^n \equiv (-1)^n\ [16]$. Or comme n est impair, on a $(-1)^n = -1$, donc $15^n \equiv -1\ [16]$. Comme $-2017 \equiv -1\ [16]$, on en déduit que $15^n \equiv -2017\ [16]$, c'est-à-dire que 16 divise $15^n + 2017$.

Propriétés : soient a et b deux entiers relatifs et n un entier naturel non nul.
1) $a - b$ divise $a^n - b^n$.
2) lorsque n est impair, $a + b$ divise $a^n + b^n$.

Démonstrations : 1) On a $a \equiv b\ [a - b]$, donc $a^n \equiv b^n\ [a - b]$, ce qui prouve que $a - b \,|\, a^n - b^n$.
2) Si n est impair, on a $a^n + b^n = a^n - (-b)^n$, qui est donc divisible par $a - (-b) = a + b$, d'après la propriété précédente.

Remarque : même si les deux propriétés précédentes se démontrent à moindre frais en utilisant les congruences, il est néanmoins utile de connaître l'identité remarquable suivante :

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k\,.$$